

# HARDWARE TOKEN WITH FINGERPRINT COLLATING FUNCTION

Publication number: JP2001357371

Publication date: 2001-12-26

Inventor: FUNABASHI TAKESHI; WADA TAKUYA

Applicant: SONY CORP

Classification:

- international: G06K9/00; G06K9/00; (IPC1-7): G06K19/073; H04L9/10

- european: G06K9/00A3

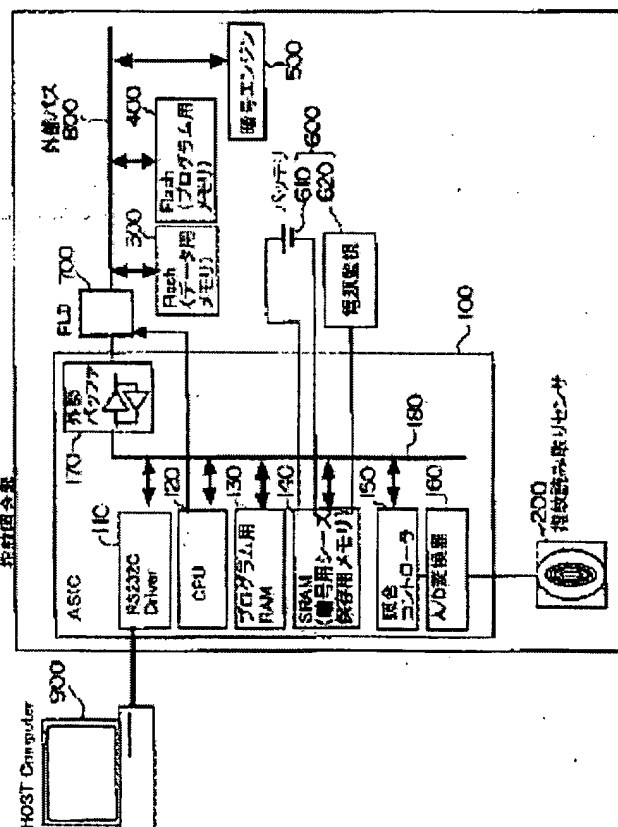
Application number: JP20000176549 20000613

Priority number(s): JP20000176549 20000613

Report a data error here

## Abstract of JP2001357371

**PROBLEM TO BE SOLVED:** To realize great tamper resistance technique at a comparatively low cost when an H/T using a PKI in a fingerprint collator is made merchandise. **SOLUTION:** When a power source is supplied, a picture is read from a fingerprint reading sensor 200 and the random number is preserved in an SRAM 140 in an ASIC 100 as a cipher key (for example, a DES key with 56 bits) for seizing a cipher. A data storing flash memory 300, a program storing flash memory 400 and a cipher engine part 500 are arranged at the outside of the ASIC 100. A fingerprint template or important data such as a PKI key are stored in the data storing flash memory 300. The cipher engine part 500 enciphers important data stored in the flash memory 300 through the use of the cipher key which is preserved in the SRAM 140 and also decodes data to be read from the flash memory 300.



Data supplied from the esp@cenet database - Worldwide

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号  
特開2001-357371  
(P2001-357371A)

(43) 公開日 平成13年12月26日 (2001. 12. 26)

(51) Int.Cl.<sup>7</sup>  
G 0 6 K 19/073  
H 0 4 L 9/10

識別記号

F I  
G 0 6 K 19/00  
H 0 4 L 9/00

テーマコード(参考)  
P 5 B 0 3 5  
6 2 1 A 5 J 1 0 4

審査請求 未請求 請求項の数17 O L (全 12 頁)

(21) 出願番号 特願2000-176549(P2000-176549)

(22) 出願日 平成12年6月13日 (2000. 6. 13)

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72) 発明者 船橋 武

東京都品川区北品川6丁目7番35号 ソニ

ー株式会社内

(72) 発明者 和田 拓也

東京都品川区北品川6丁目7番35号 ソニ

ー株式会社内

Fターム(参考) 5B035 AA13 BA05 BB09 BC01 CA11  
CA12 CA38

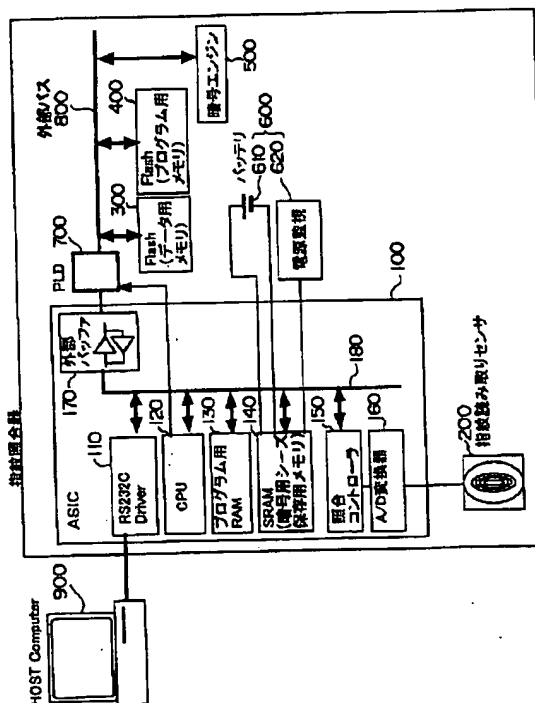
5J104 AA45 JA13 KA17 NA02 NA35  
NA37 NA38 NA42

(54) 【発明の名称】 指紋照合機能付きハードウェアトークン

(57) 【要約】

【課題】 指紋照合器にPKIを使ったH/Tの商品化に際して、強力なタンパレジスタンス技術を比較的低コストで実現する。

【解決手段】 電源が投入されたとき、指紋読み取りセンサ200から画像読み取りを行い、その乱数を暗号用シーズである暗号鍵(例えば56bitのDESキー)としてASIC100内のSRAM140に保存する。また、ASIC100の外部にデータ格納用フラッシュメモリ300と、プログラム格納用フラッシュメモリ400と、暗号エンジン部500を設ける。そして、データ格納用フラッシュメモリ300には指紋テンプレートやPKI鍵等の重要データを格納する。また、暗号エンジン部500により、SRAM140に保存した暗号鍵を用いて、フラッシュメモリ300に記憶する重要データの暗号化を行い、またフラッシュメモリ300から読み出すデータの復号化を行う。



【特許請求の範囲】

【請求項1】 カード型ケースの内部に指紋照合器を構成するメインICを設けるとともに、前記ケースに指紋読み取りセンサを設けた指紋照合機能付きハードウェアトークンであって、

前記メインIC内に設けられ、暗号用シーズを保存するための第1メモリ手段と、

前記メインICの外部に設けられ、PKI鍵及び指紋テンプレートを含む重要データを保存するための第2メモリ手段と、

前記メインICの外部に設けられ、前記重要データを前記暗号用シーズによって暗号化して前記第2メモリ手段に格納するとともに、前記第2メモリ手段に格納した重要データを前記暗号用シーズによって復号化する暗号化エンジン手段と、

前記メインICの外部バスを介して前記第1メモリ手段内の暗号用シーズがソフトウェアによって読み出されようとした場合に、前記第1メモリ手段の暗号用シーズを破壊する第1データ漏洩防止手段と、

前記ケースの機械的加工及び解体された場合に、前記第1メモリ手段の暗号用シーズを破壊する第2データ漏洩防止手段と、

を有することを特徴とする指紋照合機能付きハードウェアトークン。

【請求項2】 前記メインICはASICより構成されていることを特徴とする請求項1記載の指紋照合機能付きハードウェアトークン。

【請求項3】 前記第1メモリ手段は、SRAM、EEPROM、フラッシュメモリ、またはプログラマブルロジックデバイスを用いることを特徴とする請求項1記載の指紋照合機能付きハードウェアトークン。

【請求項4】 前記暗号化にはDESによる暗号化法を用いることを特徴とする請求項1記載の指紋照合機能付きハードウェアトークン。

【請求項5】 前記暗号用シーズは、電源投入時における指紋読み取りセンサの検出信号を検出し、この検出信号によって生成した乱数をDES鍵として用いることを特徴とする請求項4記載の指紋照合機能付きハードウェアトークン。

【請求項6】 前記乱数をバックアップのために1回だけ外部メモリ手段への記録を行うようにしたことを特徴とする請求項5記載の指紋照合機能付きハードウェアトークン。

【請求項7】 前記第1メモリ手段に記憶した乱数が前記メインICの外部バスを介してモニタすることでは読み取れないように、メインICと外部バスとのアイソレーションを行うバッファ手段を設けたことを特徴とする請求項5記載の指紋照合機能付きハードウェアトークン。

【請求項8】 前記第2メモリ手段に格納された重要デ

ータの読み出しは、前記指紋照合器による照合の結果、指紋の一致が判定された場合に許可することを特徴とする請求項1記載の指紋照合機能付きハードウェアトークン。

【請求項9】 前記第1データ漏洩防止手段は、前記第1メモリ手段内の情報を内部ソフトウェアを書き換えて読み出そうとする行為に対して前記第1メモリ手段の暗号用シーズをソフトウェア的に破壊することを特徴とする請求項1記載の指紋照合機能付きハードウェアトークン。

【請求項10】 前記第2データ漏洩防止手段は、前記第1メモリ手段がSRAMである場合に、前記SRAMへの通電を停止することにより、暗号用シーズをハードウェア的に破壊することを特徴とする請求項1記載の指紋照合機能付きハードウェアトークン。

【請求項11】 前記ケースを構成するカバーを固定するためのネジを前記SRAMへの通電手段に使用することにより、前記ネジを取り外した時点で前記SRAMへの通電が停止して暗号用シーズが破壊されるようにしたことを特徴とする請求項10記載の指紋照合機能付きハードウェアトークン。

【請求項12】 前記ケースに前記SRAMへの通電を行うための配線パターンを設け、前記ケースに孔を開けた時点で前記配線パターンが破壊され、前記SRAMへの通電が停止して暗号用シーズが破壊されるようにしたことを特徴とする請求項10記載の指紋照合機能付きハードウェアトークン。

【請求項13】 前記ケース内に前記SRAMへの通電を行うための配線パターンを設けたシートを配置し、前記ケースの破損またはケースを構成するカバーの開放によって前記シートが破損し、前記SRAMへの通電が停止して暗号用シーズが破壊されるようにしたことを特徴とする請求項10記載の指紋照合機能付きハードウェアトークン。

【請求項14】 前記ケースを構成するカバーの開放を検出する検出手段を有し、前記第2データ漏洩防止手段は、カバーの開放が検出された時点で前記第1メモリ手段の暗号用シーズを破壊することを特徴とする請求項1記載の指紋照合機能付きハードウェアトークン。

【請求項15】 前記外部バスのコントロールを行うプログラマブルロジックデバイスを有し、不正行為を感知した時点で、バスコントロールを破壊することにより、内部データの漏洩防止を行うことを特徴とする請求項1記載の指紋照合機能付きハードウェアトークン。

【請求項16】 前記ケース内にプリント基板上の回路素子を覆うプロテクトシートを設け、前記プロテクトシートの導体シートのショートを検出した時点で前記第1メモリ手段の暗号用シーズを破壊することを特徴とする請求項1記載の指紋照合機能付きハードウェアトークン。

【請求項１７】 前記ケース内の配線にグルーチップを挿入し、前記プロテクトシートと接着することにより、前記プロテクトシートを開放してグルーチップの導線が切断されたことを検出した時点で前記第１メモリ手段の暗号用シーズを破壊することを特徴とする請求項１６記載の指紋照合機能付きハードウェアトークン。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】 本発明は、各種の電子商取引等に用いられるＩＣカード等のハードウェアトークンに関し、特に不正使用防止機能を強化した指紋照合機能付きハードウェアトークンに関する。

【０００２】

【従来の技術】 例えばインターネット等を使用した電子商取引は、今後一般化されることが予想され、この普及に伴って、暗証コードの盗用等による犯罪も当然のことながら増加することが予想される。これらの犯罪を未然に防ぐために、ＰＫＩ（公開鍵暗号法）による暗号鍵（秘密鍵、公開鍵）を埋め込んだＩＣカード（スマートカードともいう）等の記憶処理装置（いわゆるハードウェアトークン、以下、Ｈ／Ｔという）が実用化されようとしている。しかしながら、このようなＨ／Ｔにおいても、Ｈ／Ｔ内に設けた暗号鍵が破られると、システム全体が破壊されることになる。このため、犯罪を未然に防ぐために、各研究機関（企業等）において、色々なタンパレジスタンス（不正防止）技術を模索しているのが現状である。

【０００３】

【発明が解決しようとする課題】 ところで、上述のようなＨ／Ｔにおけるタンパレジスタンスを考えた場合に、一般的には、タンパレジスタンスを強化すればするほど、Ｈ／Ｔのコストが高くなる。また、従来のＩＣカードにおいて、ＣＰＵと暗号化ＬＳＩ、及び暗号アルゴリズム用のメモリを１チップ化して、ＩＣカード内に埋め込んだ製品が提供されているが、このような１チップ化した場合、全ての処理を同一チップ内で扱うことになり、データの暗号化や復号化に時間がかかるという問題や、メモリ容量の制限から暗号鍵の拡張時の障害となるといった問題があった。さらに、暗号アルゴリズムの変更や鍵長のアップグレードの際に、設計を全面的にやり直さなければならないという問題もあった。

【０００４】 そこで本発明の目的は、特に指紋照合器にＰＫＩを使ったＨ／Ｔの商品化に際して、強力なタンパレジスタンス技術を比較的低コストで実現できる指紋照合機能付きＨ／Ｔを提供することにある。

【０００５】

【課題を解決するための手段】 本発明は前記目的を達成するため、カード型ケースの内部に指紋照合器を構成するメインＩＣを設けるとともに、前記ケースに指紋読み取りセンサを設けた指紋照合機能付きＨ／Ｔであって、

前記メインＩＣ内に設けられ、暗号用シーズを保存するための第１メモリ手段と、前記メインＩＣの外部に設けられ、ＰＫＩ鍵及び指紋テンプレートを含む重要データを保存するための第２メモリ手段と、前記メインＩＣの外部に設けられ、前記重要データを前記暗号用シーズによって暗号化して前記第２メモリ手段に格納するとともに、前記第２メモリ手段に格納した重要データを前記暗号用シーズによって復号化する暗号化エンジン手段と、前記メインＩＣの外部バスを介して前記第１メモリ手段内の暗号用シーズがソフトウェアによって読み出されようとした場合に、前記第１メモリ手段の暗号用シーズを破壊する第１データ漏洩防止手段と、前記ケースの機械的加工及び解体された場合に、前記第１メモリ手段の暗号用シーズを破壊する第２データ漏洩防止手段とを有することを特徴とする。

【０００６】 本発明の指紋照合機能付きＨ／Ｔにおいて、メインＩＣ内の第１メモリ手段には暗号用シーズが保存され、メインＩＣの外部に設けられた第２メモリ手段にはＰＫＩ鍵及び指紋テンプレートを含む重要データが保存される。また、メインＩＣの外部に設けられた暗号化エンジン手段は、上述した重要データを暗号用シーズによって暗号化して第２メモリ手段に格納し、逆に第２メモリ手段に格納した重要データを暗号用シーズによって復号化する。このように第２メモリ手段と暗号化エンジン手段をメインＩＣの外側に設けたため、暗号化等に伴うメインＩＣの負担を減らすことができ、また、暗号アルゴリズムの変更や鍵長のアップグレード等の際に、メインＩＣ側の設計変更を簡略でき、容易に設計変更を行うことができる。また、メインＩＣ内の第１メモリ手段に格納した暗号用シーズは、第１、第２データ漏洩防止手段により、ハードとソフトの両面から不正に読み取られることを防止し、強力なタンパレジスタンスを行うことができる。

【０００７】

【発明の実施の形態】 以下、本発明による指紋照合機能付きＨ／Ｔ（ハードウェアトークン）の実施の形態について説明する。図１は、本発明の実施の形態による指紋照合機能付きＨ／Ｔの構成を示すブロック図である。本例の指紋照合機能付きＨ／Ｔ（指紋照合器）は、メインＩＣとしてのＡＳＩＣ１００と、指紋読み取りセンサ２００と、データ格納用フラッシュメモリ３００と、プログラム格納用フラッシュメモリ４００と、暗号エンジン部５００と、電源電池６１０及び電源監視回路６２０を有する電源バッテリー部６００と、ＰＬＤ（プログラマブルロジックデバイス）７００と、外部バス８００を有する。

【０００８】 また、ＡＳＩＣ１００は、ＲＳ２３２Ｃデバイス１１０と、ＣＰＵ１２０と、プログラム用ＲＡＭ１３０と、暗号用シーズ保存用のＳＲＡＭ１４０と、照合コントローラ１５０と、Ａ／Ｄ変換器１６０と、外部

バッファ170と、内部バス180とを有する。このようなASIC100において、RS232Cデバイス110は、RS232CによってASIC100とホストコンピュータ900とのインターフェイスをとるものである。また、CPU120は、この指紋照合器全体をコントロールするものであり、プログラム用RAM130は、プログラム用ワーキングRAM130である。

【0009】また、SRAM140は、フラッシュメモリ300内のデータを暗号化するための暗号用シーズを保存するメモリである。外部バッファ170は、ASIC100内の内部バス180の内容がモニタできないようにするため、内部バス180と外部バス800とのアイソレーションを行うものである。照合コントローラ150は、指紋の照合を行うエンジン部である。A/D変換器160は、指紋読み取りセンサ200からのアナログ画像データをデジタルデータに変換するものである。

【0010】このASIC100からは、外部バッファ170を介して外部バス800が出ており、その外部バス800に上述したデータ格納用フラッシュメモリ300と、プログラム格納用フラッシュメモリ400と、暗号エンジン部500と、PLD700が接続されている。データ格納用フラッシュメモリ300は、指紋用テンプレート、PKI鍵ペア（プライベート（秘密）鍵、パブリック（公開）鍵）等の重要データが保存されている。また、プログラム格納用フラッシュメモリ400は、各種プログラムが保存されている。また、暗号エンジン部500は、PKI鍵の生成と暗号化・復号化を行うものである。

【0011】また、電源バッテリー部600は、電源電池610及び電源監視回路620で構成されている。電源電池610は、SRAM140のバックアップ電源であり、指紋照合器の電源が切れても内部データの保存を行うためのものである。電源監視回路620は、指紋照合器の電源を監視するデバイスであり、電源が切れた状態をASIC100に知らせることで、バッテリーからの消費電力を小さく押さえるためのものである。また、PLD700は、ASIC100の内部バス180と外部バス800との間で信号のやりとりを制御するものである。

【0012】以上のような構成の指紋照合器は、以下の機能を有する。

(1) 指紋画像の読み取り・指紋テンプレートの保存・指紋照合機能

(2) ホストコンピュータからのデータの書き込み・読み出し・保存（保存に際しては、DESによる暗号化を伴う）機能

(3) PKI鍵の発生と保存・PKI鍵による暗号化・復号化機能

(4) 乱数の発生と乱数に基づくDES鍵による暗号化・復号化機能

(5) (4)にて作成されたDES鍵の保存機能

【0013】次に、本例における指紋照合器の動作について順に説明する。

(2) 一般的動作の説明

図2は、本例における指紋照合器の各動作を示すフローチャートであり、以下、このフローチャートを適宜用いて説明する。

(2-1)、初期動作（暗号用シーズ作成）

本例の指紋照合器に初めて電源が投入されたとき、すなわちSRAM140内がオール0を検出すると（製造出荷時に0にしておく）、内部CPU120は、指紋読み取りセンサ200から、画像読み取りを行う（指が置いてない状態での読み取りのためのノイズ画像を読み取る）。このデータは、読み取り毎に常に異なる値になり（温度・湿度・電源・その他の環境差）、この値が乱数として使えることは、実験から証明済みである。そこで、この乱数値を、暗号鍵（例えば56bitのDESキー）としてSRAM140に保存する（図2（A）のステップS1、S2）。なお、SRAM140内のデータを暗号鍵として使う際に、外部から外部バス800をモニタしても読むことができないように、バスアイソレーション用に外部バッファ170が入っている。

【0014】(2-2) 指紋の登録（ホストコンピュータ900からの指示で行う）

指を指紋読み取りセンサ200に置き、指紋画像を取り込む。これをA/D変換器160が2値画像に変換し、照合コントローラ150に送る。照合コントローラ150は、このデータ内の特徴部（いわゆるテンプレートという）を抽出し、SRAM140に保存されている暗号鍵（56bitのDESキー）で暗号化し、フラッシュメモリ300に保存される（図2（B）のステップS11、S12）。

【0015】(2-3) 指紋の照合（ホストコンピュータ900からの指示で行う）

指を指紋読み取りセンサ200に置き、指紋画像を取り込む。これをA/D変換器160が2値画像に変換する。照合コントローラ150では、先ほど登録した、テンプレートと指紋照合を行う。この結果がOK（照合一致）になると、以下のことが実行できるモードになる（なお、ホストコンピュータ900の指示により、このモードの解除ができる）。

(A) 指紋の再登録

(B) PKI暗号鍵ペアの作成

(C) PKI暗号鍵の内、秘密鍵の使用が可能になる。

(D) データ用フラッシュメモリ300内に記録する際にDES鍵により暗号化する。また読み出しの際には復号化する。

【0016】(2-4) PKI暗号鍵ペアの作成（ホストコンピュータ900からの指示で行う）

指紋照合がOK（照合一致）になった時点で、PKIの

鍵を作成する。作成された鍵をSRAM140に保存されている暗号鍵(56bitのDESK)で暗号化し、フラッシュメモリ300に記録する(図2(C)のステップS21、S22、S23)。次に、この際、外部バス800上に配置されている暗号エンジン部500を使用するために、一般的に秘密鍵が外部バス800上に現れる(外部バス800をモニタすることで秘密鍵を盗むことが可能となる)。しかし、この行為ができるのは本人(指紋照合の結果が一致の人)のみであることから問題は生じないものである。

【0017】(2-5)PKI暗号鍵を使ったファイルの暗号化

次に、本例の暗号化についてファイル暗号を例に説明する。まず、ホストコンピュータ900内で、あるファイルFを暗号化する場合、ホストコンピュータ900は、指紋照合器から乱数R(これをDESKとして使用する)を読み出す。そして、このkを使い、ファイルFをDESK暗号方式にて暗号化(F)<sup>k</sup>する(図2(D)のステップS31、S32)。次に、このkを、さらに指紋照合器から読み出したPKIの公開鍵eで暗号化(k)<sup>e</sup>する(図2(D)のステップS33)。

【0018】(2-6)PKI暗号鍵を使ったファイルの復号化

次に、本例の復号化についてファイル復号を例に説明する。上述のようにして暗号化されたファイル(F)<sup>k</sup>を復号する場合、指紋照合がOKになった時点で、ホストコンピュータ900は(k)<sup>e</sup>を指紋照合器に送り込む。指紋照合器内で秘密鍵dを使い復号し、DESK鍵kを取り出してホストコンピュータ900に送り返す(図2(E)のステップS41)。このDESK鍵kを使い、ファイル(F)<sup>k</sup>を復号しFを復元させる(図2(E)のステップS42)。

【0019】(3)SRAM140への電力供給  
(3-1)基本的な考え方。

SRAM140に保存されたDESK鍵を使い、重要なデータ(例えば、テンプレートや秘密鍵)を暗号化してから、フラッシュメモリ300に記録する。フラッシュメモリ300内のデータを盗むためには、SRAM140に保存されたDESK鍵を初めに取り出す必要がある。しかしながら、本例では、以下に示すような各種の漏洩防止手段によってSRAM140への電源を切ることはできず(内部データが破壊する)、さらに、ソフトウェア的に取り出すことも困難にし、不正防止を行うようにしている。

【0020】(3-2)SRAM140への電源供給  
図3は、本例の指紋照合器におけるケースに設けられた電源供給用の配線構造を具体的に示す図であり、図3(A)がケースを構成する上カバー10の内面図、図3(B)がケースを構成する上カバー10と下カバー20とプリント基板30を示す分解側面図、図3(C)がケ

ースを構成する下カバー20の上面図である。なお、プリント基板30上には、各種回路が配置されているが、ここではSRAM140と電池610に関して説明する。

【0021】また、プリント基板30は、上カバー10と下カバー20に挟まれており、上カバー10と下カバー20は、4本のネジ40で固定されている。この固定ネジ40が下カバー20の孔22Aを通り、プリント基板30と接触しており、かつ下カバー20のA点では、プリント基板30の配線により電池610の+側につながっている。このネジ40は、上カバー10に設けたナット12に螺合する。そして、上カバー10のA'点のナット12とB'点のナット12とは、パターン配線14によりカバー10の内部で互いに接続されている。

【0022】同様に、下カバー20のB点のネジ40は、上カバー10のB'点のナット12に接続される。また、下カバー20のB点は、プリント基板30のパターン配線32を介してSRAM140の+側に接続されている。したがって、上カバー10と下カバー20がネジ40で固定されると、パターン配線14がB点のネジ40を介してSRAM140の+側に接続される。一方、電池610の-側は、プリント基板30のパターン配線32を介してSRAM140の-側に接続されていることから、SRAM140に対しての電力が供給される。図4(A)は、このような配線構造を模式的に示す回路図である。

【0023】(3-3)データ詐取

以上のような構造から本指紋照合器の稼働後に、内部データを盗もうとカバーを取り外すために、A点もしくはB点のネジ40を取り外した時点で、SRAM140への通電経路が破壊され、その内部に保存されているDESK鍵が破壊することになる。なお、本例では、A点とB点の2本のネジ40で、SRAM140への通電経路を確保しているが、もっと多くの接点を設けても良い。図4(B)は、図3(C)に示す4つの点A、B、C、Dの各ネジ40で通電経路を確保した場合の配線構造を模式的に示す回路図である。

【0024】(4)ソフトウェアの書き換え

(4-1)上記の例は、メカニカルにSRAM140内のデータを詐取する場合に対応する方法について説明したが、外部からファームウェアを書き換えることでSRAM140内データを詐取することも考えられる。しかしながら、本例では、ホストコンピュータ900からファームウェアを書き換えるためのコマンドが発行された時点で、SRAM140内のデータ(DESK鍵)がソフト的に破壊されるようになっている。これにより、外部からのファームウェアの書き換えによるデータ詐取を阻止することができる。

【0025】(5)初期動作においてSRAM140内へのDESK鍵保存

(5-1) 上述のような仕組みにより、SRAM140内のデータ、及びフラッシュメモリ300内の重要データの詐取をきわめて難しくすることができるが、逆に、電池610切れや、修理等によりカバーを外す場合に、本人でさえ重要データの読み出しができなくなる問題が出てくる。そこで、(2-1)においてSRAM140に乱数を保存した直後に、1回だけ、例えばフロッピディスク等の外部メモリ手段に同じデータをバックアップとして保存する。このバックアップ処理は、ソフトウェアでコントロールする。また、バックアップをとったことを示す印(フラグ等)をSRAM140上に記録する。そして、この印がある場合は、2度とバックアップはとれないようにする。

【0026】(5-2) 電池610が切れた場合の交換時の対応として、図4(A)に示すように、電池610と平行にコンデンサ630を配置しておく。電池交換時の短時間は、このコンデンサからSRAM140への電源供給を行う。

【0027】以上のように、本例によれば、ASIC100内に非常に少ない容量(56ビットのDESキーである場合、8バイトで良い)のSRAM140を配置し、暗号エンジン部500をASIC100の外部に配置することにより、ASIC100の変更を行うことなく、比較的容易に暗号アルゴリズムの変更や、鍵長変更が可能になる。さらに、データ保存用フラッシュメモリ(秘密鍵や指紋テンプレート保存用)300をASIC100の外部に配置することにより、ASIC100に影響を及ぼすことなく、重要データの大きさに制限がなくなり、自在に機能拡張等を行うことが可能となる。さらに指紋照合器とPKIを組み合わせたハードウェアトークンという商品化において、各種のデータ漏洩防止手段により、強力なタンパレジスタンス機能を提供することが可能となる。

【0028】次に、本実施の形態における応用例について説明する。

#### (6) 応用例1

(6-1) カバーを外さずに孔開け等の不正な加工を行う方法への対応(図5)

上述のようなケースの構造においてカバー10、20を外さずに孔を開けることにより、プリント基板30上の外部バスをモニタすることで、SRAM140内のデータを盗み出す方法が考えられる。そこで、図5(A)に示すように各カバー10、20の内面に1本の線を蛇行させて形成したパターン配線(本例ではメッシュ配線という)16、26によって、カバー10、20に孔を開けた時点で、SRAM140への電源供給を切る方法である。上述した例と同様にプリント基板30は、上カバー10と下カバー20に挟まれており、上カバー10と下カバー20は、4本のネジ40で固定されている。固定ネジ40が、下カバー20の孔22Aを通り、プリン

ト基板30と接触しており、かつ下カバー20のA点では、プリント基板30のパターン配線32により電池610の+側につながっている。

【0029】このネジ40は、上カバー10に設けたナット12に螺合する。そして、上カバー10のA'点から上カバー10内の配線16により、D'点に接続されている。下カバー20のD点のネジ40が、A点同様に固定されるとプリント基板30の配線32により、D点とC点が接続される。そして、C点のネジ40を介してプリント基板30に接続され、このC点からプリント基板30の配線32により、SRAM140の+側に接続される。SRAM140の-側は、プリント基板30の配線32により、電池610の-側に接続されている。さらに電源供給ラインとして、A点がプリント基板30の配線により電池610のプラスにつながっている。これにより、SRAM140に対しての電力が供給される。

【0030】(6-2) プリント基板30上の電池610、ASIC100、及び外部バス800の露出部にメッシュシートを付加する方法(図6)

このメッシュシート50は、4本のネジ42でプリント基板30上に取り付けられる。プリント基板30上のA点からメッシュシート50上のパターン配線52によりD点に接続され、D点からC点はプリント配線により接続され、C点からB点はメッシュシート50上の配線54により接続されている。そして、SRAM140の-側は電池610の-側にプリント配線により接続され、B点からSRAM140の+側に接続されている。したがって、メッシュシート50がネジ42で固定されると、SRAM140への電源供給が行われる。そして、メッシュシート50を外すか、孔を開けた時点でSRAM140への電源供給が切れることになる。

【0031】(6-3) 電池610の代わりにコンデンサを使う

上述した例では、ボタン電池610を想定しているが、これに限らずリチャージャブルな電池やコンデンサによってバックアップすることも可能である。

#### 【0032】(7) 応用例2

(7-1) EEPROMによるタンパレジスタンス技術  
上述した例では、SRAM140を使用する例を説明したが、ASIC100内にSRAM140の代わりにEEPROMやフラッシュメモリを使うことも考えられる。この場合、電池610は必要なくなり、上述のような通電停止によるデータの破壊を行うことはできないが、この場合には例えば次の応用例2を採用することができる。

【0033】(7-2) 上述した(6)の方法(通電停止)と全く逆の方法で積極的に破壊(図7)

上述した応用例1では、電池610からの電源を常に入れておくことを利用してデータの漏洩防止を図ったが、

逆にカバー（ケース）を開けた時に、内蔵電池610がONになり、それをセンスしたCPU120がSRAM140の代わりに設けたフラッシュメモリやEEPROM内のデータ（SRAM140の場合と同様にDES鍵が保存されている）を破壊する方法も考えられる。これは、図7に示すように、上カバー10を開けると、リリースピン60が持ち上がり、電池（ボタン電池）610に板ばねよりなるばね接点62が接触する。これにより、例えばホストコンピュータ900からの電源が切れていても、指紋照合器への電源が入り、かつそれをセンスしたCPU120がフラッシュメモリ、EEPROM内のデータ（乱数によるDES鍵）を破壊する。この場合のメリットは、常時通電が必要なSRAMを使わないことにより、電池610の消耗を大幅に改善できるとともに、適正な電池交換操作ではデータを破壊しないため、電池交換時を含めて誤って通電を停止してしまい、データを破壊してしまうことも極めて少なくなる。

#### 【0034】（7-3）PLDの破壊（図8）

上述したPLD700内に前もって、外部バス800のコントローラを内蔵しておく。そして、カバーが外された時点で、CPU120によってコントローラを破壊する。それ以後、全体的に動作不能になる。さらに、図8に示すように、PLD700内のメモリ710に上述した乱数（DES鍵）、あるいは、DESの暗号アルゴリズムも入れておく。これにより、カバーが取り外された際に、PLD700内のデータを破壊することも考えられる。

#### 【0035】（8）応用例3

（8-1）上述した図3～図6に示したデータ漏洩防止手段では、ケースを構成するカバーを取り外したり、孔を開けることにより、SRAM140への通電経路が壊れ、内部のデータを破壊するようにしたが、この場合、通電経路を構成するネジ40の間をケースの外側で導線によって接続した後、カバーの一部を破壊したり、カバーに孔を開けたりすることにより、内部のプリント基板30上の外部バスをモニタすることで、SRAM140内のデータを盗み出す方法が考えられる。もちろん、上述した図3～図6の方法では、タンパエビデンス（不正に破壊した証拠を残す）としては有効があるが、完全なタンパレジスタンス（不正防止）としては、さらに改良の余地のあるものである。

【0036】また、上述した例では、フラッシュメモリへのプログラムロード時には、ソフト的に内部データを破壊することで、偽物のソフトウェアロードによる乱数読み出し犯罪を防いでいる。しかし、この場合、上述した上カバーやメッシュシートを取り去った後に、プリント基板上のフラッシュメモリを偽物のプログラムが記憶されているフラッシュメモリに物理的に交換し、SRAM内の乱数を読み出すことが可能となる。そこで、以下の応用例3では、このようなケースの外部に導線を設け

るような巧妙な不正行為に対しても、データ漏洩を防止する手段について説明する。

【0037】（8-2）プロテクトシート構造（図9）  
プロテクトシート70は、2枚の導体シート（全面に導体膜が行き渡ったシート形状のもので配線ではない）72A、72Bを、数ミクロン（例えば2 $\mu$ m）という非常に薄く、かつ、柔らかい絶縁フィルム74で電気的に分離した構造を有する。また、さらに各導体シート72A、72Bの外側全面を保護シート76A、76Bによって挟んだ構造となっている。そして、このようなプロテクトシート70を切断、あるいは孔開けした場合には、絶縁フィルム74による絶縁状態が壊れ、導体シート72A、72Bが電気的に導通することになる。したがって、このようなプロテクトシート70をカバー10、20の内側等に配置し、各導体シート72A、72Bの導通状態をASIC100で監視することにより、カバー10、20の不正な加工を検出し、内部データの破壊を行うようにする。

【0038】（8-3）グルーチップ構造（図10）  
グルーチップ80は、適当な大きさを有するプラスチックモールド部品82A、82Bで、1本の導線（銅線）84を埋め込んだものである。この導線84の両端がプラスチックモールド部品82A、82Bから外側に延出しており、プリント基板上で配線の一部を担うものである。したがって、このようなグルーチップ80をプリント基板30の配線に挿入することにより、ケースに不正な加工が加えられた場合の導線84の分断を検出でき、内部データの破壊を行うようにする。

【0039】（8-4）全体構造の具体例（図11）  
製造組み立ての方法として、図11に示すように、ASIC100とフラッシュメモリ300/400の中間と外側に合計3つのグルーチップ80が配置されている。そして、グルーチップ80の上部にエポキシ樹脂系等の接着剤90が塗布され、その上面にプロテクトシート70が配置される。プロテクトシート70は、4つのコーナ部A、B、C、Dをプリント基板30の上面にネジ止めまたは半田付け等によって取り付けられている。

#### 【0040】（8-5）回路の構成

プロテクトシート70及びグルーチップ80は、それぞれプリント基板30の配線に接続されている。まず、プリント基板30上で、電池の+電極は図11のA点に配線されており、A点からプロテクトシート70の+側導体シート72Bにネジまたは半田により接続されている。さらに、+側導体シート72BはC点に接続されている。そして、このC点からネジを介してプリント基板30上の配線に接続され、その後、3つのグルーチップ80を介してSRAM140の+側に配線されている。次に、電池の-電極がB点に配線されており、B点からプロテクトシート70の-側導体シート72Aにネジまたは半田によって接続されている。さらに、この-側導



体シート72Aは、D点に接続されており、このD点からプリント基板30の配線を介してSRAM140の一侧に接続されている。

#### 【0041】(8-6) 犯罪行為

以上のような構成において、例えば上述したA点とC点を導体で接続し、さらにB点とD点を接続し、その後、プロテクトシート70をはがそうとすると、グルーチップ80がプロテクトシート70側に接着剤90で接着されているため、外れてしまい、電気回路的に切断されることになる。したがって、これをASIC100側で検出し、SRAM140内のデータを破壊する。また、プロテクトシート70に孔を開けたり、切断した場合には、+側と-側がショートし、やはりSRAM140内のデータを破壊する。なお、データ漏洩防止手段の具体的な構成としては、上述した例に限らず、例えばカバーの開放を検出する手段として各種のセンサ等が考えられることから、これらセンサ等と上述した各種の方法を組み合わせるように構成し得ることはもちろんである。

#### 【0042】

【発明の効果】以上説明したように本発明の指紋照合機能付きH/Tは、メインIC内に設けられ、暗号用シーズを保存するための第1メモリ手段と、メインICの外部に設けられ、PKI鍵及び指紋テンプレートを含む重要データを保存するための第2メモリ手段と、メインICの外部に設けられ、重要データを暗号用シーズによって暗号化して第2メモリ手段に格納するとともに、第2メモリ手段に格納した重要データを暗号用シーズによって復号化する暗号化エンジン手段と、メインICの外部バスを介して第1メモリ手段内の暗号用シーズがソフトウェアによって読み出されようとした場合に、第1メモリ手段の暗号用シーズを破壊する第1データ漏洩防止手段と、ケースの機械的加工及び解体された場合に、第1メモリ手段の暗号用シーズを破壊する第2データ漏洩防止手段とを有することを特徴とする。

【0043】このため、本発明の指紋照合機能付きH/Tでは、第2メモリ手段と暗号化エンジン手段をメインICの外側に設けたため、暗号化等に伴うメインICの負担を減らすことができ、また、暗号アルゴリズムの変更や鍵長のアップグレード等の際に、メインIC側の設計変更を簡略でき、容易に設計変更を行うことができる。また、メインIC内の第1メモリ手段に格納した暗号用シーズは、第1、第2データ漏洩防止手段により、ハードとソフトの両面から不正に読み取られることを防止し、強力なタンパレジスタンスを行うことができる。したがって、指紋照合器にPKIを使ったH/Tの商品化に際して、強力なタンパレジスタンス技術を比較的低コストで実現できる指紋照合機能付きH/Tを提供する

ことができる効果がある。

#### 【図面の簡単な説明】

【図1】本発明の実施の形態による指紋照合機能付きH/Tの構成例を示すブロック図である。

【図2】図1に示す指紋照合機能付きH/Tの各動作を示すフローチャートである。

【図3】図1に示す指紋照合機能付きH/Tの配線パターンの一例を示す図であり、図3(A)は上カバーの内面図、図3(B)は上下カバーとプリント基板の分解側面図、図3(C)は下カバーの内面図である。

【図4】図4(A)は図3に示す配線パターンの模式的に示す回路図、図4(B)は図4(A)の変形例を示す回路図である。

【図5】図1に示す指紋照合機能付きH/Tの配線パターンの他の例を示す図であり、図5(A)は上カバーの内面図、図5(B)は上下カバーとプリント基板の分解側面図、図5(C)は下カバーの内面図である。

【図6】図1に示す指紋照合機能付きH/Tの配線パターンのさらに他の例を示す平面図である。

【図7】図1に示す指紋照合機能付きH/Tのケースの開放を検出する構成を示す図であり、図7(A)は上下カバーとプリント基板の分解側面図、図7(B)は回路図である。

【図8】図1に示す指紋照合機能付きH/Tに設けたPLDの構成例を示すブロック図である。

【図9】図1に示す指紋照合機能付きH/Tに設けるプロテクトシートの一例を示す図であり、図9(A)は平面図、図9(B)は側断面図である。

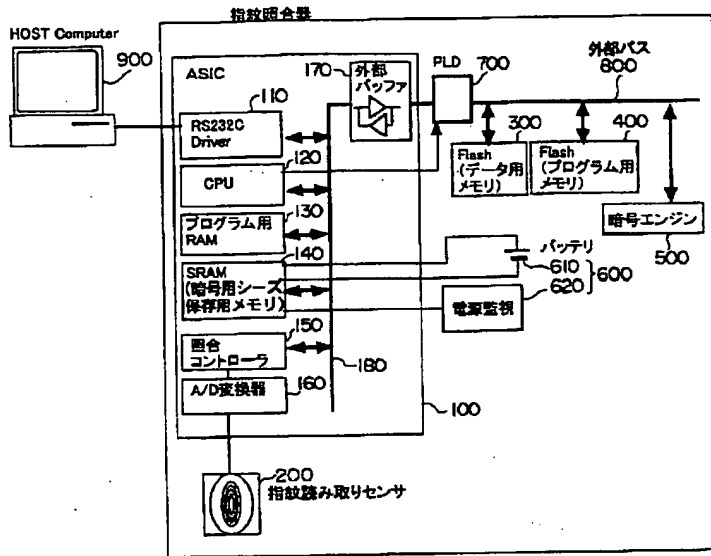
【図10】図1に示す指紋照合機能付きH/Tに設けるグルーチップの一例を示す側面図である。

【図11】図9に示すプロテクトシートと図10に示すグルーチップを指紋照合機能付きH/Tのプリント基板上に設けた例を示す平面図である。

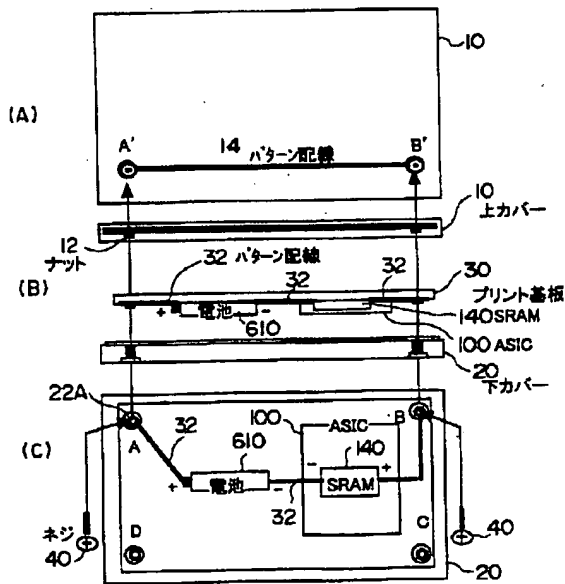
#### 【符号の説明】

10…上カバー、20…下カバー、30…プリント基板、40…ネジ、100…ASIC、110…RS232Cデバイス、120…CPU、130…プログラム用RAM、140…暗号用シーズ保存用SRAM、150…照合コントローラ、160…A/D変換器、170…外部バッファ、180…内部バス、200…指紋読み取りセンサ、300…データ格納用フラッシュメモリ、400…プログラム格納用フラッシュメモリ、500…暗号エンジン部、600…電源バッテリー部、610…電源電池、620…電源監視回路、700…PLD、800…外部バス、900…ホストコンピュータ。

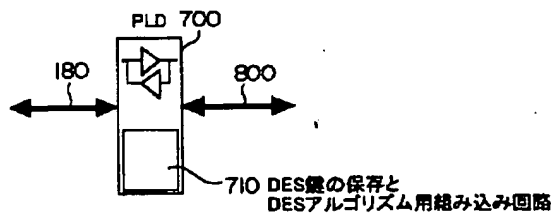
【図1】



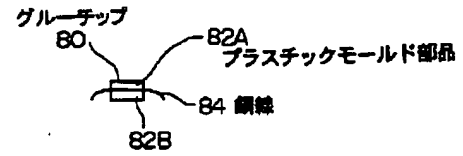
【図3】



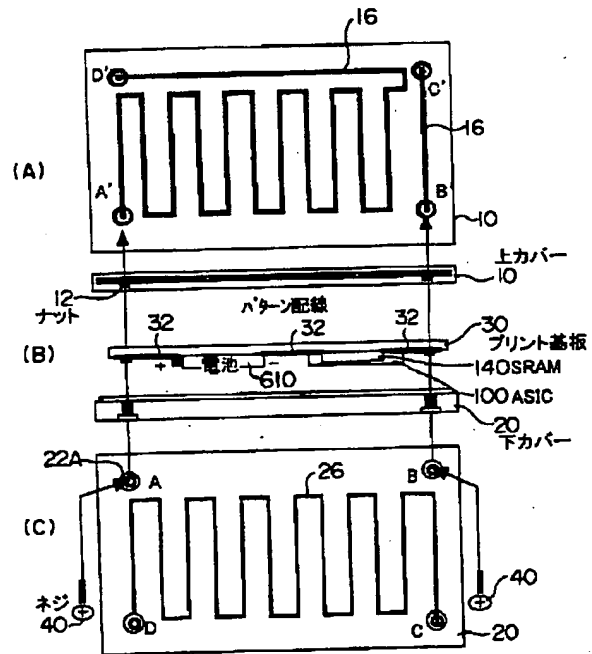
【図8】



【図10】

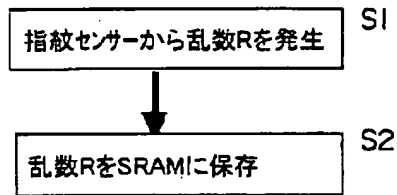


【図5】

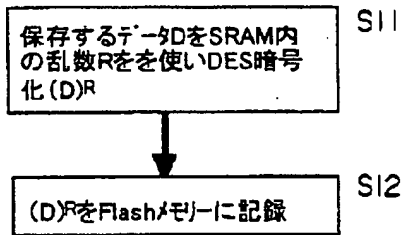


【図2】

A) 乱数の発生と保存

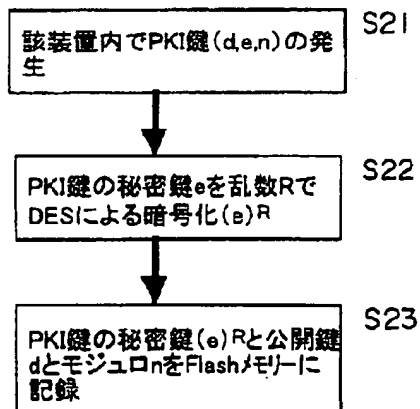


B) Flashメモリーへのデータ保存



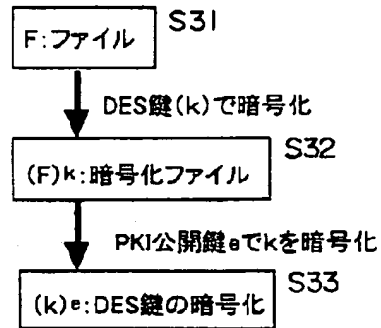
データ Dの一例:  
 \* 指紋テンプレート  
 \* PKIの秘密鍵

C) PKI鍵の発生と保存

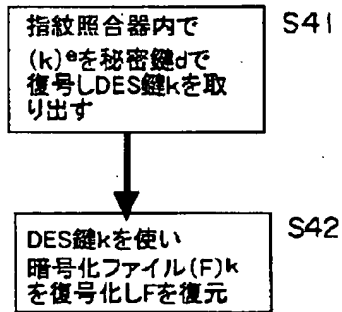


e: 秘密鍵  
 d: 公開鍵  
 n: モジュロ

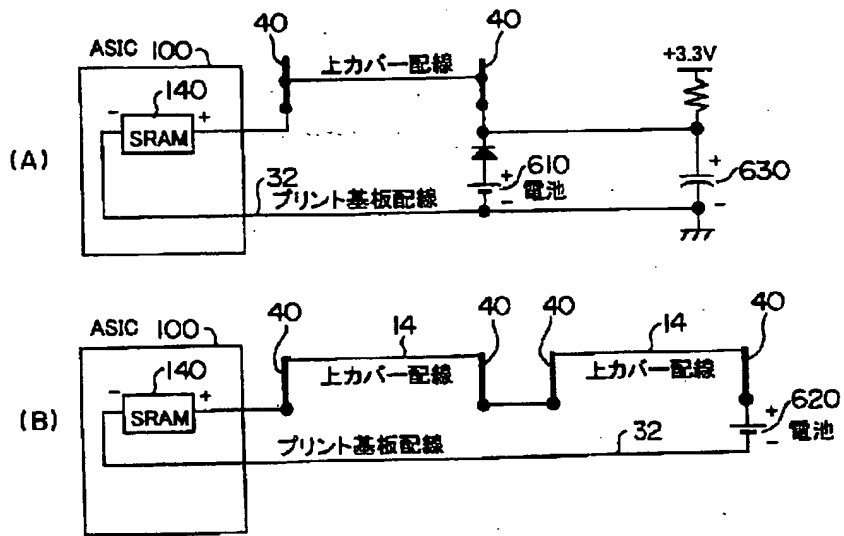
D) ファイルの暗号化例



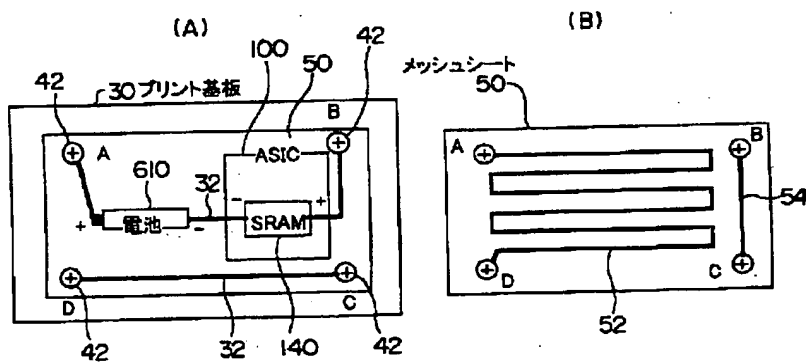
E) ファイルの復号化例



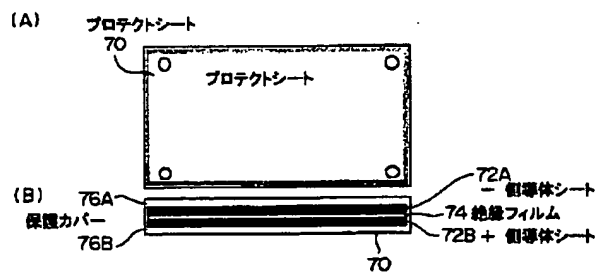
【図4】



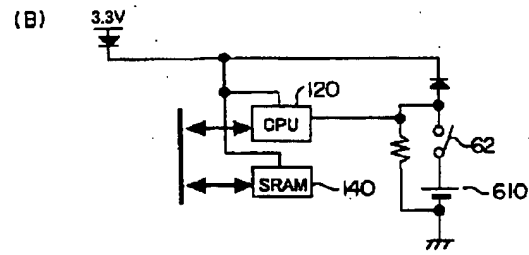
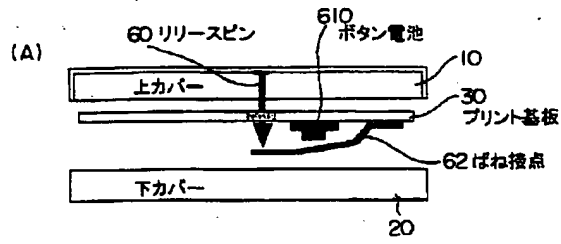
【図6】



【図9】



【図7】



【図11】

